REMARKS/ARGUMENTS

In the Office action dated September 15, 2005, claims 1 - 22 were rejected under 35 U.S.C. § 103. By this Amendment, Applicant has amended the specification, amended claims 1, 6, 8, 10 and 15, and added claims 23 and 24. Reconsideration and reexamination are hereby requested for claims 1 - 24 that are now pending in this application.

Applicant's Amendments to the Specification and Claims

Applicant has amended the specification and claims to correct several informalities. Applicant submits that no new matter has been added as the amendments are supported by the context of the original disclosure.

Response to the 35 U.S.C. § 103 Rejection of the Claims

Claims 1, 5 - 7 and 16 - 22 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Silverbrook at al., U.S. Patent No. 6,334,190 (hereafter referred to as "Silverbrook"), in view of an article by Sait et al. (hereafter referred to as "Sait"). Claims 1 and 10 are independent. Claims 5 - 7 depend on claim 1. Claims 16 - 22 depend on claim 10.

Dependent claims 2, 8, 9 and 13 - 15 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Silverbrook in view of Sait, and further in view of a book by Schneier (hereafter referred to as "Schneier").

Dependent claims 3, 4 and 12 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Silverbrook in view of Sait, and further in view of Yokota et al., U.S. Patent No. 6,304,657 (hereafter referred to as "Yokota").

Independent claim 1 recites, in part: "a hash engine configured to implement hash round logic for a SHA1 authentication algorithm . . . including, a combined adder tree with a timing critical path having a single 32-bit carry look-ahead adder (CLA)." Independent claim 10 recites, in part: "processing the fixed-size data blocks using a SHA-1 multi-round authentication engine architecture, said architecture implementing hash round logic for a SHA1 authentication algorithm including a combined adder tree with a timing critical path having a single 32-bit carry look-ahead adder (CLA)."

Silverbrook discloses the conventional HMAC-SHA1 algorithm. In the implementation of this hashing algorithm, XORing and addition operations are performed on the data. See column 11, lines 9 - 29 and column 42.

Sait discloses a technique for fast multiplications. See Sait's Abstract and Introduction on page 109. Sait is not directed to authentication or any other form of cryptography.

In rejecting claims 1 and 10 the Office action states, in part, that "Sait teaches a plurality of adder trees with a timing critical path having a single carry-ahead adder to perform multiplication in cryptographic operations" and that it would have been obvious to combine Silverbrook's system and Sait's technique resulting in "a combined adder having a single CLA."

However, neither the claimed apparatus and method nor the hashing algorithms disclosed in Silverbrook involve multiplication operations. Hence, one skilled in the art looking to improve hash operations would not have been motivated to use Sait which teaches how to improve multiplication times. Moreover, there would have been no motivation for one skilled in the art looking to improve the cryptographic techniques of Silverbrook to consider Sait because Sait is not directed to the field of cryptography.

As just explained above, there is no suggestion in either reference or in the art or any motivation to combine these references. Even if the two were combined, their combination would not disclose or suggest the claimed invention. For example, the cited references to not teach or suggest that hash round logic for a SHA1 authentication algorithm may include a combined adder tree with a timing critical path having a single 32-bit carry look-ahead adder as claimed. Sait says nothing regarding a timing critical path or the use of a single 32-bit carry look-ahead adder, much less that it would be feasible or advantageous to use this in conjunction with hash round logic for a SHA1 authentication algorithm.

Applicant thus submits that claims 1 and 10 are not obvious over Silverbrook in view of Sait. Claims 2 - 9 and 11 - 24 that depend on claims 1 or 10 also are patentable over the cited references for the reasons set forth above. In addition, these claims are patentable over the cited references for the additional limitations that these claims contain.

For example, claim 2 recites that "a timing critical path equivalent to one of: one 5-bit addition, one 32-bit CSA, a multiplexer operation, and one 32-bit CLA; and three 32-bit

CSAs, a multiplexer operation, and one 32-bit CLA." Schneier cited in the Office action merely discusses the conventional SHA algorithm. There is no mention of the specifically claimed structure that as discussed in the specification may be advantageously used for a timing critical path of a hash round logic implementation. Moreover, there is no mention or suggestion of the use of a multiplexer operation as claimed.

There is no teaching or suggestion to incorporate the specific structure and relationship to the combiner adder tree set forth in claim 3. None of the cited references, including Yokota, teach or suggest that a SHA1 authentication algorithm could or may advantageously be implemented using a 5-bit circular shifter preceding the claimed combined adder tree (from claim 1).

Similarly, there is no teaching that the combiner adder tree includes add5to1 and add4to1 adders as set forth in claim 4. The portion of Yokota cited in the Office action merely discloses shifting and XOR operations and states that other operations such as add and carry may be used instead. Yokota does not, however, mention the specifically claimed add5to1 and add4to1 adders. Moreover, there is no teaching or suggestion that the claimed combined adder tree (from claim 1) may be implemented using such adders.

Regarding claim 5 the cited portions of Sait make no mention of round operations, much less "addition computations are conducted in parallel with round operations" as claimed.

Claim 6 is directed to an authentication engine architecture that more effectively processes a multi-round algorithm by providing specific structure that enables concurrent processing. In particular, claim 6 recites two separate hash engines:

> a first instantiation of a SHA-1 authentication algorithm hash round logic in an inner hash engine;
>
> a second instantiation of a SHA-1 authentication algorithm hash round logic in an outer hash engine;

Moreover, claim 6 also recites specific structure that enables the multiple hash engines to operate concurrently. For example, claim 6 recites:

> a dual-frame payload data input buffer configured for loading one new data block while another data block one is being processed in the inner hash engine;
>
> an initial hash state input buffer configuration for loading initial hash states to the inner and outer hash engines for concurrent inner hash and outer hash operations; and
>
> a dual-ported ROM configured for concurrent constant lookups for both inner and outer hash engines.

In contrast, Silverbrook discloses use of the standard HMAC algorithm and discloses a technique for reducing the number of registers used in a SHA1 algorithm. Silverbrook does not teach or suggest the use of concurrent multi-round hash operations as claimed.

Regarding claim 8, the cited portions of Schneier merely mention that constants may be reused. The same number of rounds (80) is still performed. Accordingly, Schneier does not teach or suggest that "eighty rounds of a SHA1 loop are collapsed into forty rounds" as claimed.

Claim 17 recites, in part:

> pipeline hash operations of said inner hash and outer hash engines,
>
> collapse and rearrange multi-round logic to reduce rounds of hash operations, and
>
> implement multi-round logic such that addition computations are conducted in parallel with round operations.

Here, the Office action cites Silver brook at col. 11 and Sait at Figures 3 and 6 and page 110. However, as discussed above, neither of the cited reference teach or suggest the use of two separate hash engines. Also as discussed above, Col. 11 merely describes the conventional HMAC algorithm. This algorithm is not inherently a pipelined operation. Silverbrook makes no other mention of pipeline operations. Moreover, the cited passages make no mention of any logic to reduce rounds of hash operations, much less the claimed "collapse and rearrange multi-round logic."

Similarly, the cited passages make no mention of pipelining involving parallel inner and outer hash operations for different payloads as claimed in claim 19. Nor do the cited passages teach or suggest the use of a dual-frame input buffer for a hash engine as set forth in claim 20, double buffering for concurrent inner and outer hash operations as set forth in claim 21, or a dual-ported ROM as set forth in claim 22.

CONCLUSION

In view of the above it is submitted that the claims are patentably distinct over the cited references and that all the rejections to the claims have been overcome. Reconsideration and reexamination of the above Application is requested.

Respectfully submitted,
CHRISTIE, PARKER & HALE, LLP

By
Stephen D. Burbach
Reg. No. 40,285
626/795-9900

SDB/vsj
VSJ PAS646292.1-*-10/3/05 4:43 PM